DRAFT Mapping Between DOE Electric Sector Cybersecurity Risk Management Maturity Initiative and High-Level Security Requirements from NISTIR 7628, *Guidelines for Smart Grid Cyber Security*

Electric Sector Cybersecurity Risk Management Maturity Initiative	NISTIR 7628, *Guidelines for Smart Grid Cyber Security* High-Level Security Requirement
Asset, Change, and Configuration Management (ASSET)	
• MIL 1	
1. Asset Inventory	SG.CM8 Component Inventory
2. Configuration Management	SG.CM-1 Configuration Management Policy and Procedures SG.CM-11 Configuration Management Plan
3. Change Management	SG.CM-1 Configuration Management Policy and Procedures SG.CM-11 Configuration Management Plan
• MIL 2	
1. Asset Inventory	SG.CM8 Component Inventory
2. Configuration Management	SG.CM-1 Configuration Management Policy and Procedures SG.CM-11 Configuration Management Plan
3. Change Management	SG.CM-1 Configuration Management Policy and Procedures SG.CM-11 Configuration Management Plan
4. Plan	SG.CM-11 Configuration Management Plan
5. Stakeholders	SG.CM-1 Configuration Management Policy and Procedures SG.PM-8 Management Accountability
• MIL 3	
1. Asset Inventory	SG.CM8 Component Inventory
2. Configuration Management	SG.CM-1 Configuration Management Policy and Procedures SG.CM-11 Configuration Management Plan
3. Change Management	SG.CM-1 Configuration Management Policy and Procedures SG.CM-11 Configuration Management Plan
4. Cross-Domain Coordination	SG.PM-8 Management Accountability
5. Policy	SG.CM-1 Configuration Management Policy and Procedures SG.CM-11 Configuration Management Plan

6. Resources	
7. Personnel	
Workforce Management (WORKFORCE)	
• MIL 1	
1. Cybersecurity Responsibilities	SG.PM-8 Management Accountability SG.SC-19 Security Roles
2. Managing workforce cybersecurity	SG.PS-1 Personnel Security Policy and Procedures SG.PS-3 Personnel Screening
3. Cybersecurity Knowledge, Skills, and Abilities	SG.AT-3 Security Training SG.AT-5 Security Responsibility Training
4. Cybersecurity Awareness	SG.AT-2 Security Awareness SG.AT-3 Security Training SG.AT-5 Security Responsibility Training
• MIL 2	
1. Cybersecurity Responsibilities	SG.PM-8 Management Accountability SG.SC-19 Security Roles
2. Managing workforce cybersecurity	SG.PS-1 Personnel Security Policy and Procedures SG.PS-3 Personnel Screening
3. Cybersecurity Knowledge, Skills, and Abilities	SG.AT-3 Security Training SG.AT-5 Security Responsibility Training
4. Cybersecurity Awareness	SG.AT-2 Security Awareness SG.AT-3 Security Training SG.AT-5 Security Responsibility Training
5. Plan	SG.AT-1 Awareness and Training Policy and Procedures SG.AT-7 Planning Process Training
6. Stakeholders	SG.AT-1 Awareness and Training Policy and Procedures SG.PM-8 Management Accountability
• MIL 3	
1. Cybersecurity Responsibilities	SG.PM-8 Management Accountability SG.SC-19 Security Roles
2. Managing workforce cybersecurity	SG.PS-1 Personnel Security Policy and Procedures SG.PS-3 Personnel Screening
3. Cybersecurity Knowledge, Skills, and Abilities	SG.AT-3 Security Training SG.AT-5 Security Responsibility Training
4. Cybersecurity Awareness	SG.AT-2 Security Awareness SG.AT-3 Security Training SG.AT-5 Security Responsibility Training

5. Policy	SG.AT-1 Awareness and Training Policy and Procedures
6. Resources	
7. Personnel	
Identity and Access Management (ACCESS)	
• MIL 1	
1. Identity Management	SG.IA-2 Identifier Management SG.IA-3 Authenticator Management SG.IA-4 User Identification and Authentication SG.IA-5 Device Identification and Authentication
2. Access Management	SG.AC-3 Account Management SG.AC-4 Access Enforcement
• MIL 2	
1. Identity Management	SG.IA-2 Identifier Management SG.IA-3 Authenticator Management SG.IA-4 User Identification and Authentication SG.IA-5 Device Identification and Authentication
2. Access Management	SG.AC-3 Account Management SG.AC-4 Access Enforcement
3. Plan	
4. Stakeholders	SG.AC-1 Access Control Policy and Procedures SG.IA-1 Identification and Authentication Policy and Procedures SG.PM-8 Management Accountability
• MIL 3	
1. Identity Management	SG.IA-2 Identifier Management SG.IA-3 Authenticator Management SG.IA-4 User Identification and Authentication SG.IA-5 Device Identification and Authentication
2. Access Management	SG.AC-3 Account Management SG.AC-4 Access Enforcement
3. Cross-domain coordination	SG.PM-8 Management Accountability
4. Policy	SG.AC-1 Access Control Policy and Procedures SG.IA-1 Identification and Authentication Policy and Procedures
5. Resources	
6. Personnel	
Risk Management (RISK)	
• MIL 1	

1. Risk Strategy	SG.PM-5 Risk Management Strategy
2. Sponsorship	SG.PM-3 Security Management Authority
3. Risk Management Program	
• MIL 2	
1. Risk Strategy	SG.PM-5 Risk Management Strategy
2. Sponsorship	SG.PM-3 Security Management Authority
3. Risk Management Program	SG.PM-2 Security Program Plan SG.PM-5 Risk Management Strategy
4. Plan	SG.RA-2 Risk Management Plan
5. Stakeholders	SG.PM-3 Security Management Authority SG.PM-8 Management Accountability
• MIL 3	
1. Risk Strategy	SG.PM-5 Risk Management Strategy
2. Risk Management Program	SG.PM-2 Security Program Plan SG.PM-5 Risk Management Strategy
3. Cross-domain coordination	SG.PM-8 Management Accountability
4. Policy	SG.AC-1 Access Control Policy and Procedures SG.AC-2 Remote Access Policy and Procedures
5. Personnel	SG.PM-8 Management Accountability
Supply Chain and External Dependencies Management (DEPENDENCIES)	
• MIL 1	
1. Dependency identification	SG.SA-11 Supply Chain Protection
2. Risk management	
3. Cybersecurity Requirements	SG.SA-3 Life Cycle Support SG.SA-11 Supply Chain Protection
• MIL 2	
1. Dependency identification	SG.SA-11 Supply Chain Protection
2. Risk management	
3. Cybersecurity Requirements	SG.SA-3 Life Cycle Support SG.SA-11 Supply Chain Protection
4. Plan	

5. Stakeholders	SG.PM-8 Management Accountability
• MIL 3	
1. Dependency identification	SG.SA-11 Supply Chain Protection
2. Risk management	
3. Cybersecurity Requirements	SG.SA-3 Life Cycle Support SG.SA-11 Supply Chain Protection
4. Cross-domain coordination	SG.PM-8 Management Accountability
5. Policy	SG.SA-1 Smart Grid Information System and Services Acquisition Policy SG.SA-11 Supply Chain Protection
6. Resources	
7. Personnel	
Threat and Vulnerability Management (THREAT)	
• MIL 1	
1. Threat management	SG.RA-4 Risk Assessment SG.RA-6 Vulnerability Assessment and Awareness
2. Vulnerability management	SG.RA-4 Risk Assessment SG.RA-6 Vulnerability Assessment and Awareness
• MIL 2	
1. Threat management	SG.RA-4 Risk Assessment SG.RA-6 Vulnerability Assessment and Awareness
2. Vulnerability management	SG.RA-4 Risk Assessment SG.RA-6 Vulnerability Assessment and Awareness
3. Cybersecurity patch management	SG.CM-3 Configuration Change Control SG.SI-2 Flaw Remediation
4. Plan	SG.CM-3 Configuration Change Control
5. Stakeholders	SG.PM-8 Management Accountability
• MIL 3	
1. Threat management	SG.RA-4 Risk Assessment SG.RA-6 Vulnerability Assessment and Awareness
2. Vulnerability Management	SG.RA-4 Risk Assessment SG.RA-6 Vulnerability Assessment and Awareness
3. Cybersecurity patch management	SG.CM-3 Configuration Change Control SG.SI-2 Flaw Remediation

4. Cross-domain coordination	SG.AT-5 Contact with Security Groups and Organizations SG.PM-8 Management Accountability
5. Policy	SG.SI-1 Smart Grid Information System and Information Integrity Policy and Procedures
6. Resources	
7. Personnel	
Event and Incident Response, Continuity of Operations (RESPONSE)	
- MIL 1	
1. Detect cybersecurity events	SG.CM-6 Configuration Settings SG.IR-5 Incident Handling SG.PE-4 Monitoring Physical Access SG.RA-6 Vulnerability Assessment and Awareness SG.SC-16 Mobile Code SG.SC-24 Honeypots SG.SI-3 Malicious Code and Spam Protection SG.SI-4 Smart Grid Information System Monitoring Tools and Techniques SG.SI-7 Software and Information Integrity
2. Declare cybersecurity incidents	SG.IR-5 Incident Handling SG.PE-4 Monitoring Physical Access SG.RA-6 Vulnerability Assessment and Awareness SG.SC-16 Mobile Code SG.SC-24 Honeypots SG.SI-3 Malicious Code and Spam Protection
3. Respond to cybersecurity incidents	SG.IR-5 Incident Handling SG.PE-4 Monitoring Physical Access SG.RA-6 Vulnerability Assessment and Awareness SG.SC-16 Mobile Code SG.SI-3 Malicious Code and Spam Protection
4. Continuity	SG.CP-7 Alternate Storage Sites SG.CP-8 Alternate Telecommunications Services SG.CP-9 Alternate Control Center SG.CP-10 Smart Grid Information System Recovery and Reconstitution
- MIL 2	
1. Detect cybersecurity events	SG.CM-6 Configuration Settings SG.IR-5 Incident Handling SG.PE-4 Monitoring Physical Access SG.RA-6 Vulnerability Assessment and Awareness SG.SC-16 Mobile Code SG.SC-24 Honeypots SG.SI-3 Malicious Code and Spam Protection SG.SI-4 Smart Grid Information System Monitoring Tools and Techniques

	SG.SI-7 Software and Information Integrity
2. Declare cybersecurity incidents	SG.IR-5 Incident Handling SG.PE-4 Monitoring Physical Access SG.RA-6 Vulnerability Assessment and Awareness SG.SC-16 Mobile Code SG.SC-24 Honeypots SG.SI-3 Malicious Code and Spam Protection
3. Respond to cybersecurity incidents	SG.IR-5 Incident Handling SG.PE-4 Monitoring Physical Access SG.RA-6 Vulnerability Assessment and Awareness SG.SC-16 Mobile Code SG.SI-3 Malicious Code and Spam Protection
4. Continuity	SG.CP-7 Alternate Storage Sites SG.CP-8 Alternate Telecommunications Services SG.CP-9 Alternate Control Center SG.CP-10 Smart Grid Information System Recovery and Reconstitution
5. Plan	SG.CP-2 Continuity of Operations Plan
6. Stakeholders	SG.PM-8 Management Accountability
• MIL 3	
1. Detect cybersecurity events	SG.CM-6 Configuration Settings SG.IR-5 Incident Handling SG.PE-4 Monitoring Physical Access SG.RA-6 Vulnerability Assessment and Awareness SG.SC-16 Mobile Code SG.SC-24 Honeypots SG.SI-3 Malicious Code and Spam Protection SG.SI-4 Smart Grid Information System Monitoring Tools and Techniques SG.SI-7 Software and Information Integrity
2. Declare cybersecurity incidents	SG.IR-5 Incident Handling SG.PE-4 Monitoring Physical Access SG.RA-6 Vulnerability Assessment and Awareness SG.SC-16 Mobile Code SG.SC-24 Honeypots SG.SI-3 Malicious Code and Spam Protection
3. Respond to cybersecurity incidents	SG.IR-5 Incident Handling SG.PE-4 Monitoring Physical Access SG.RA-6 Vulnerability Assessment and Awareness SG.SC-16 Mobile Code SG.SI-3 Malicious Code and Spam Protection
4. Continuity	SG.CP-7 Alternate Storage Sites SG.CP-8 Alternate Telecommunications Services SG.CP-9 Alternate Control Center SG.CP-10 Smart Grid Information System Recovery and Reconstitution

5. Cross-domain	SG.PM-8 Management Accountability
6. Policy	SG.CP-1 Continuity of Operations Policy and Procedures
7. Resources	SG.CP-3 Continuity of Operations Roles and Responsibilities
8. Personnel	SG.CP-3 Continuity of Operations Roles and Responsibilities SG.CP-4 Continuity of Operations Training
Situational Awareness (SITUATION)	
• MIL 1	
1. Logging	SG.AC-8 Unsuccessful Login Attempts SG.AC-10 Previous Logon Notification SG.AU-10 Audit Record Retention SG.AU-16 Non-repudiation SG.PE-4 Monitoring Physical Access SG.PE-6 Visitor Records SG.PE-7 Physical Access Log Retention SG.SI-4 Smart Grid Information System Monitoring Tools and Techniques
2. Monitoring	SG.AC-3 Account Management SG.AC-15 Remote Access SG.AC-16 Wireless Access Restrictions SG.AC-17 Access Control for Portable and Media Devices SG.AU-6 Audit Monitoring, Analysis, and Reporting SG.CA-2 Security Assessments SG.CA-4 Smart Grid Information System Connections SG.CA-6 Continuous Monitoring SG.CM-4 Monitoring Configuration Changes SG.IR-6 Incident Monitoring SG.MA-6 Remote Maintenance SG.PE-4 Monitoring Physical Access SG.PE-5 Visitor Control SG.RA-2 Risk Management Plan SG.RA-6 Vulnerability Assessment and Awareness SG.SC-7 Boundary Protection SG.SC-16 Mobile Code SG.SC-17 Voice-Over Internet Protocol SG.SI-2 Flaw Remediation SG.SI-4 Smart Grid Information System Monitoring Tools and Techniques SG.SI-7 Software and Information Integrity
3. Awareness	SG.PM-4 Security Architecture
• MIL 2	

1. Logging	SG.AC-8 Unsuccessful Login Attempts SG.AC-10 Previous Logon Notification SG.AU-10 Audit Record Retention SG.AU-16 Non-repudiation SG.PE-4 Monitoring Physical Access SG.PE-6 Visitor Records SG.PE-7 Physical Access Log Retention SG.SI-4 Smart Grid Information System Monitoring Tools and Techniques
2. Monitoring	SG.AC-3 Account Management SG.AC-15 Remote Access SG.AC-16 Wireless Access Restrictions SG.AC-17 Access Control for Portable and Media Devices SG.AU-6 Audit Monitoring, Analysis, and Reporting SG.CA-2 Security Assessments SG.CA-4 Smart Grid Information System Connections SG.CA-6 Continuous Monitoring SG.CM-4 Monitoring Configuration Changes SG.IR-6 Incident Monitoring SG.MA-6 Remote Maintenance SG.PE-4 Monitoring Physical Access SG.PE-5 Visitor Control SG.RA-2 Risk Management Plan SG.RA-6 Vulnerability Assessment and Awareness SG.SC-7 Boundary Protection SG.SC-16 Mobile Code SG.SC-17 Voice-Over Internet Protocol SG.SI-2 Flaw Remediation SG.SI-4 Smart Grid Information System Monitoring Tools and Techniques SG.SI-7 Software and Information Integrity
3. Awareness	SG.PM-4 Security Architecture
4. Plan	
5. Stakeholders	SG.PM-8 Management Accountability
• MIL 3	
1. Logging	SG.AC-8 Unsuccessful Login Attempts SG.AC-10 Previous Logon Notification SG.AU-10 Audit Record Retention SG.AU-16 Non-repudiation SG.PE-4 Monitoring Physical Access SG.PE-6 Visitor Records SG.PE-7 Physical Access Log Retention SG.SI-4 Smart Grid Information System Monitoring Tools and Techniques

2. Monitoring	SG.AC-3 Account Management SG.AC-15 Remote Access SG.AC-16 Wireless Access Restrictions SG.AC-17 Access Control for Portable and Media Devices SG.AU-6 Audit Monitoring, Analysis, and Reporting SG.CA-2 Security Assessments SG.CA-4 Smart Grid Information System Connections SG.CA-6 Continuous Monitoring SG.CM-4 Monitoring Configuration Changes SG.IR-6 Incident Monitoring SG.MA-6 Remote Maintenance SG.PE-4 Monitoring Physical Access SG.PE-5 Visitor Control SG.RA-2 Risk Management Plan SG.RA-6 Vulnerability Assessment and Awareness SG.SC-7 Boundary Protection SG.SC-16 Mobile Code SG.SC-17 Voice-Over Internet Protocol SG.SI-2 Flaw Remediation SG.SI-4 Smart Grid Information System Monitoring Tools and Techniques SG.SI-7 Software and Information Integrity
3. Awareness	SG.PM-4 Security Architecture
4. Cross-domain coordination	SG.PM-8 Management Accountability
5. Policy	SG.SC-1 System and Communication Protection Policy and Procedures SG.SI-1 System and Information Integrity Policy and Procedures
6. Resources	
7. Personnel	
Information Sharing and Communications (SHARING)	
• MIL 1	
1. Communication	SG.AT-5 Contact with Security Groups and Organizations SG.IR-11 Coordination of Emergency Response
2. Analysis	
3. Coordination	SG.AT-5 Contact with Security Groups and Organizations SG.IR-11 Coordination of Emergency Response

• MIL 2	
1. Communication	SG.AT-5 Contact with Security Groups and Organizations SG.IR-11 Coordination of Emergency Response
2. Analysis	
3. Coordination	SG.AT-5 Contact with Security Groups and Organizations SG.IR-11 Coordination of Emergency Response
4. Plan	
5. Stakeholders	SG.PM-8 Management Accountability
• MIL 3	
1. Communication	SG.AT-5 Contact with Security Groups and Organizations SG.IR-11 Coordination of Emergency Response
2. Analysis	
3. Coordination	SG.AT-5 Contact with Security Groups and Organizations SG.IR-11 Coordination of Emergency Response
4. Policy	
5. Resources	
6. Personnel	
Cybersecurity Program Management (CYBER)	
• MIL 1	
1. Strategy	SG.PM-3 Senior Management Authority SG.PM-5 Risk Management Strategy SG.PM-7 Mission/Business Process Definition
2. Sponsorship	SG.PM-3 Senior Management Authority SG.PM-8 Management Accountability
3. Cybersecurity program	SG.PM-2 Security Program Plan SG.PM-5 Risk Management Strategy
4. Cybersecurity architecture	SG.PM-4 Security Architecture
• MIL 2	
1. Strategy	SG.PM-3 Senior Management Authority SG.PM-5 Risk Management Strategy SG.PM-7 Mission/Business Process Definition
2. Sponsorship	SG.PM-3 Senior Management Authority SG.PM-8 Management Accountability

3. Cybersecurity program	SG.PM-2 Security Program Plan SG.PM-5 Risk Management Strategy
4. Cybersecurity architecture	SG.PM-4 Security Architecture
5. Plan	SG.PM-2 Security Program Plan SG.PM-5 Risk Management Strategy
6. Secure software development	SG.SA-8 Security Engineering Principles SG.SA-9 Developer Configuration Management SG.SA10 Developer Security Testing
7. Stakeholders	SG.PM-8 Management Accountability
• MIL 3	
1. Strategy	SG.PM-3 Senior Management Authority SG.PM-5 Risk Management Strategy SG.PM-7 Mission/Business Process Definition
2. Sponsorship	SG.PM-3 Senior Management Authority SG.PM-8 Management Accountability
3. Cybersecurity program	SG.PM-2 Security Program Plan SG.PM-5 Risk Management Strategy
4. Cybersecurity architecture	SG.PM-4 Security Architecture
5. Secure software development	SG.SA-8 Security Engineering Principles SG.SA-9 Developer Configuration Management SG.SA10 Developer Security Testing
6. Policy	SG.PM-1 Security Policy and Procedures
7. Personnel	SG.SC-19 Security Roles